

## UNITED STATES DISTRICT COURT

for the  
Western District of Oklahoma**FILED**

NOV - 6 2019

CARMELITA REEDER SHIN  
CLERK, U.S. DISTRICT COURT  
BY: [Signature]  
DEPUTY

In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*Black iPhone cell phone, Model A1784, FCC ID:  
BCG-E3092A, IC:579C-E3092ACase No. MJ-19- 585 -P

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, which is incorporated by reference herein.

located in the Western District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. § 841(a)(1)	Distribution Methamphetamine, a schedule II controlled substance

The application is based on these facts:  
See attached Affidavit, which is incorporated by reference herein.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of        days (give exact ending date if more than 30 days:       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[Signature]  
*Applicant's signature*ELSA CASTRO, Task Force Officer, DEA  
*Printed name and title*

Sworn to before me and signed in my presence.

Date:

11/6/19City and state: Oklahoma City, Oklahoma[Signature]  
*Judge's signature*GARY M. PURCELL, U.S. Magistrate Judge  
*Printed name and title*

DELAWARE

AND DISTRICT OF COLUMBIA

TS/DOO TOLNEN & PALLCO  
ATTORNEYS AT LAW  
1000 K STREET, N.W.  
WASHINGTON, D.C. 20004



**ATTACHMENT A**

**DESCRIPTION OF DEVICE TO BE SEARCHED**

The property to be searched is a black iPhone Cell Phone, Model A1784, FCC ID: BCG-E3092A, IC: 579C-E3092A, hereinafter the "Device". The Device is currently located in secure evidence storage at DEA Oklahoma City located, at 901 NE 122<sup>nd</sup> Street, Ste 210, Oklahoma City, Oklahoma.

The warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

**iPhone Cell Phone, Model A1784, FCC ID: BCG-E3092A, IC: 579C-E3092A**



*Handwritten signature*  
EC

**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

1. All records on the Device described in Attachment A that relate to violations of Title 21 U.S.C. § 841 (21 U.S.C. §§ 841 (a)(1)) involving Hector Mario ESPARZA, including:
  - a. lists of customers and related identifying information including images and videos;
  - b. types, amounts, and prices of drugs smuggled as well as dates, places, and amounts of specific transactions;
  - c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
  - d. all bank records, checks, credit card bills, account information, and other financial records.
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
  - a. records of Internet Protocol addresses used;
  - b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

A handwritten signature in black ink, appearing to be "EMB" with "EC" written below it.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

*amb*  
EC

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF A  
BLACK IPHONE CELL PHONE, MODEL  
A1784, FCC ID: BCG-E3092A, IC:579C-  
E3092A, CURRENTLY LOCATED IN  
SECURE EVIDENCE STORAGE AT THE  
DEA OFFICE IN OKLAHOMA CITY, OK

Case No. \_\_\_\_\_

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Elsa Castro, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property— electronic Device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been a Peace Officer since September 2012. I am currently employed by the Oklahoma Bureau of Narcotics and Dangerous Drugs Control (hereinafter referred to as OBNDD) as a full-time Peace Officer and Narcotics Agent and have been employed since September 24, 2012. In July 2018, I was assigned to Drug Enforcement Agency (hereinafter referred to as DEA) HIDTA in Oklahoma City, Oklahoma and continue to work in that assignment on the date of this affidavit.

3. My experience includes but is not limited to participating in debriefs relating to narcotics investigations, conducting physical surveillance, conducting English and Spanish interviews, and monitoring wiretaps. I have also acted in an undercover capacity where I have purchased drugs in hand-to-hand transactions with drug dealers. I am familiar with techniques and operations of those involved in the drug trade and their day-to-day activities. I have also monitored on court-ordered wiretap investigations, conspiracies, and “common” street level buys where telephone communications were intercepted that involved the distribution of controlled dangerous substances. This activity included both the observations of audio calls and text messages on numerous occasions. I have received training in narcotics investigations such as the Basic CLEET Academy, OBNDD Narcotics Investigators School, Advanced Vehicle Contraband Concealment Course, Basic Clandestine Laboratory Safety and Site Safety Officer, Advanced Undercover Techniques and Survival for Women, and Exploitation of Stored Internet Communication Records and Real Time Intercept Capabilities, as well as courses dealing with the importation of narcotics from the southwest border of the United States and the realities of undercover operations.

4. I have participated in numerous investigations involving individuals who have been involved and have personal knowledge of transporting and concealing narcotics, as well as, the amassing, spending, converting, transporting, distributing, laundering and concealing of proceeds from narcotics trafficking and smuggling.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

**IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

6. The property to be searched is a black iPhone Cell Phone, Model A1784, FCC ID: BCG-E3092A, IC: 579C-E3092A, hereinafter the "Device." The Device is currently located in secure evidence storage at DEA Oklahoma City, located at 901 NE 122<sup>nd</sup> Street, Ste 210, Oklahoma City, Oklahoma.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

**PROBABLE CAUSE**

8. The Device were seized incident to arrest from Hector Mario **ESPARZA** for a violation of 21 U.S.C. § 841 (a)(1), Distribution of Methamphetamine, a Schedule II controlled substance.

9. The purpose of the following affidavit is to provide probable cause to support a search of Hector Mario **ESPARZA** phone and to establish he violated 21 U.S.C.



§ 841 (a)(1), Distribution of Methamphetamine, a Schedule II controlled substance. Since this affidavit is being submitted for the limited purpose of establishing probable cause for the search of the Device, I have not included each and every known fact regarding the instant investigation. More specifically, I have set forth only pertinent facts that I believe are necessary to establish probable cause that **ESPARZA** committed the violation of 21 U.S.C. § 841 (a)(1) and used as an instrumentality the Device as outlined below.

#### **FACTS SUPPORTING PROBABLE CAUSE**

10. On October 17, 2019, an arrest warrant was issued by the United States District Court, Western District of Oklahoma, for **ESPARZA** for the Distribution of Methamphetamine, a Schedule II controlled substance, a violation of 21 U.S.C. § 841 (a)(1).

11. On November 1, 2019, **ESPARZA** was arrested by members of the DEA OKC HITDA group. **ESPARZA** was at his place of employment, Lopez Foods located at 9500 N.W. 4<sup>th</sup> Street, Oklahoma City, Oklahoma. The Device was seized incident to arrest from **ESPARZA's** locker located at his place of employment. The Lopez Foods security personnel indicated that each employee had their own locker. The Lopez Foods Security personnel retrieved the Device, **ESPARZA's** wallet and keys from **ESPARZA's** locker.

12. On November 1, 2019, DEA OKC HITDA members assisted United States Probation Officers conduct a search of **ESPARZA's** residence. **ESPARZA** is currently on federal probation. During the search, probation offices and DEA agents located approximately 621.8 gross grams of methamphetamine in the master bedroom dresser drawer.

13. A presumptive field test on a sample of the methamphetamine was conducted with positive results confirming the presence of methamphetamine.

14. The Device is currently located in secure evidence storage at DEA Oklahoma City, located at 901 NE 122<sup>nd</sup> Street, Ste 210, Oklahoma City, Oklahoma. In my training and experience, I know that the Device have been stored in a manner in which its contents are (to the extent material to this investigation) in substantially the same state as they were when the Device first came into the possession of DEA.

15. Based on my training, experience, and research; I know that the Device has capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on a Device of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

16. From my training and experience, I know that drug smuggling is often a conspiratorially crime. Individuals who possess controlled substances with the intent to

deliver them typically do so in groups with the assistance of others. Drug smugglers often use their cell phones to communicate with other members of the drug trafficking organization. Records of these communications and the contact information of the smugglers are often saved in the individual's phone.

17. An examination can reveal the approximate location of the Device and the user by associating a specific date and time with: historical GPS data, historical cell-site data, and logs of Wi-Fi networks. Additionally, an examination can reveal the Device unique identifiers (phone number, IMEI, IMSI, etc.). These unique identifiers can be used to compel material records from the cell phone service provider such as call logs, billing information, and historical cell-site data.

18. From my training and experience, I know it is common for individuals who illegally possess controlled substances to conceal the contraband in secure locations within their residence, motor vehicles, and other real property over which they have dominion and control.

### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

19. Based on my knowledge, training, and experience, I know that electronic Device can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This

information can sometimes be recovered with forensics tools.

20. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic Device were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other

evidence also falls within the scope of the warrant.


- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

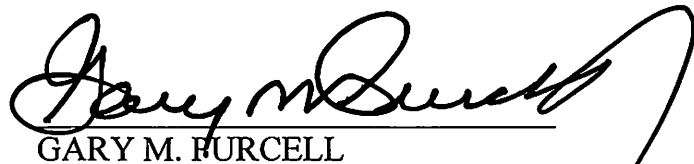
23. *Manner of execution.* Because this warrant seeks only permission to examine a Device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

**CONCLUSION**

24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

  
ELSA CASTRO  
Task Force Officer  
Drug Enforcement Administration

SUBSCRIBED AND SWORN to before me on this 6<sup>th</sup> day of November 2019.

  
GARY M. FURCELL  
United States Magistrate Judge



**ATTACHMENT A**

**DESCRIPTION OF DEVICE TO BE SEARCHED**

The property to be searched is a black iPhone Cell Phone, Model A1784, FCC ID: BCG-E3092A, IC: 579C-E3092A, hereinafter the "Device". The Device is currently located in secure evidence storage at DEA Oklahoma City located, at 901 NE 122<sup>nd</sup> Street, Ste 210, Oklahoma City, Oklahoma.

The warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

**iPhone Cell Phone, Model A1784, FCC ID: BCG-E3092A, IC: 579C-E3092A**



EC *[Signature]*

**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

1. All records on the Device described in Attachment A that relate to violations of Title 21 U.S.C. § 841 (21 U.S.C. §§ 841 (a)(1)) involving Hector Mario ESPARZA, including:

- a. lists of customers and related identifying information including images and videos;
- b. types, amounts, and prices of drugs smuggled as well as dates, places, and amounts of specific transactions;
- c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
- d. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

EC  
gmb

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

EC  
jmb